Uncovering a broad criminal ecosystem powered by one of the largest botnets, Glupteba

Wednesday 28 September 2022, 12:00 - 12:30

Luca Nagy (Google)

Botnets continue to be a serious threat against companies and individuals worldwide. However, little is known about exactly how botnets are monetized and how revenues flow to criminal actors. Our research uncovers a whole criminal network of organizations behind a one million sized botnet, named Glupteba.

The Glupteba botnet rose to our attention after being downloaded tens of thousands of times per day through traffic distributors and pay-per-install networks. The botnet is known to steal user credentials and cookies from infected hosts, mine cryptocurrencies and deploy and operate proxy components. Given the botnet's size, its technical sophistication and the wide range of functionality provided by the botnet, we decided to map out the ecosystem and understand the incentives and functioning of this underground economy to better disrupt it and build better defences in the future. Our investigation led us to uncover a complex ecosystem formed by the botnet, its operators and victims and the customers of the various illicit services provided by the botnet. For instance, a cookie theft service aimed at abusing advertising networks including Google, Facebook and Twitter (dontfarm), a proxy provider giving botnet customers the ability to proxy traffic through victim machines (awmproxy), or a service which sells credit card numbers to be used for malicious activities such as purchasing malicious ads or conducting payment fraud (extracard). The Glupteba ecosystem is one of the most complex we have witnessed that also supports multiple platforms. We have identified and analysed multiple components used by the Glupteba actors. We will share details of many of them, including proxy and ad fraud components running on Windows and IOT devices. Our year-long study of this broad ecosystem led to novel findings and attributions that led to disruption and legal actions undertaken against the Glupteba operators.

In this presentation we will walk through our in-depth investigations starting with the botnet’s distribution techniques, its capabilities and how each capability was monetized in this broad criminal ecosystem.

Luca Nagy

Luca Nagy is a security engineer at Google, Threat Analysis Group in Zurich. She completed her studies in computer engineering, during which she developed an interest in IT security and a passion for malware analysis. Then at SophosLabs, Luca spent her time reverse engineering emerging threats and creating detections against them. In 2020 she joined Google to focus on understanding and disrupting serious financially motivated threats against Google and Google's users.

@luca_nagy_ (https://twitter.com/luca_nagy_)

BACK TO VB2022 PROGRAMME PAGE (/CONFERENCE/VB2022/PROGRAMME)

Other VB2022 papers

The threat is stronger than the execution: realities of hacktivism in the 2020s (/conference/vb2022/abstracts/threat-stronger-execution-realities-hacktivism-2020s/)

VB2022 paper: The threat is stronger than the execution: the realities of hacktivism in the 2020s

Uncovering a broad criminal ecosystem powered by one of the largest botnets, Glupteba (/conference/vb2022/abstracts/uncovering-broad-criminal-ecosystem-powered-one-largest-botnets-glupteba/)

VB2022 paper: Uncovering a broad criminal ecosystem powered by one of the largest botnets, Glupteba

Zeroing in on XENOTIME: analysis of the entities responsible for the Triton event (/conference/vb2022/abstracts/zeroing-xenotime-analysis-entities-responsible-triton-event/)

VB2022 paper: Zeroing in on XENOTIME: analysis of the entities responsible for the Triton event

Prilex: the pricey prickle credit card complex (/conference/vb2022/abstracts/prilex-pricey-prickle-credit-card-complex/)

VB2022 paper: Prilex: the pricey prickle credit card complex

Exploit archaeology: a forensic history of in-the-wild NSO Group exploits (/conference/vb2022/abstracts/exploit-archaeology-forensic-history-wild-nso-group-exploits/)

VB2022 paper: Exploit archaeology: a forensic history of in-the-wild NSO Group exploits

Hunting the Android/BianLian botnet (/conference/vb2022/abstracts